

IN THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A method of capturing a security breach, comprising:
deploying a honey pot;
detecting a breach of the honey pot, wherein the breach indicates the honey pot has been compromised;
capturing a state of the honey pot, including by creating a copy of data associated with the honey pot as compromised; and
automatically redeploying the honey pot, including by reinitializing the state of the honey pot.
2. (Original) The method of claim 1, further including analyzing the breach.
3. (Original) The method of claim 1, further including automatically analyzing the breach.
4. (Original) The method of claim 1, wherein the breach is automatically detected.
5. (Canceled)
6. (Original) The method of claim 1, further including shutting down the honey pot.
7. (Original) The method of claim 1, further including configuring the honey pot.
8. (Currently Amended) The method of claim 1, ~~further including~~ wherein capturing the state comprises copying a honey pot image.
9. (Original) The method of claim 1, wherein the honey pot is a physical machine.
10. (Original) The method of claim 1, wherein the honey pot is a virtual machine.
11. (Canceled)
12. (Canceled)
13. (Original) The method of claim 1, wherein detecting is based on the number of outgoing connections detected.
14. (Original) The method of claim 1, wherein detecting is based on the number of incoming connections detected.
15. (Original) The method of claim 1, wherein detecting is based on an elapsed time.
16. (Canceled)

17. (Original) The method of claim 1, wherein the honey pot runs a Linux operating system.
18. (Original) The method of claim 1, further including saving state information associated with the honey pot.
19. (Original) The method of claim 1, further including saving state information associated with the honey pot and wherein saving and redeploying occur in parallel.
20. (Original) The method of claim 1, further including analyzing the breach and wherein analyzing and redeploying occur in parallel.
21. (Original) The method of claim 1, further including:
 - receiving an incoming connection associated with an IP address;
 - mapping the IP address to the honey pot; and
 - releasing the IP address mapping.
22. (Original) The method of claim 1, further including:
 - receiving an incoming connection associated with an IP address;
 - mapping the IP address to the honey pot;
 - releasing the IP address mapping; and
 - mapping another IP address to the honey pot.
23. (Currently Amended) A computer program product for capturing a security breach, the computer program product being embodied in a computer readable medium and comprising computer instructions for:
 - deploying a honey pot;
 - detecting a breach of the honey pot, wherein the breach indicates the honey pot has been compromised;
 - capturing a state of the honey pot, including by creating a copy of data associated with the honey pot as compromised; and
 - automatically redeploying the honey pot, including by reinitializing the state of the honey pot.
24. (Currently Amended) A system for capturing a security breach, comprising:
 - a processor configured to:
 - deploy a honey pot;
 - detect a breach of the honey pot, wherein the breach indicates the honey pot has been compromised;

capture a state of the honey pot, including by creating a copy of data associated with the honey pot as compromised; and

automatically redeploy the honey pot, including by reinitializing the state of the honey pot; and

a memory coupled with the processor, wherein the memory provides the processor with instructions.